UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/668,026	09/21/2000	William T. Jennings	064751.0298	8477

7590 04/09/2004

Baker Botts LLP
2001 Ross Avenue
Dallas, TX 75201-2980

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	PAPER NUMBER
2131	7

DATE MAILED: 04/09/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

7

4

Office Action Summary	**Application No.** 09/668,026	**Applicant(s)** JENNINGS, WILLIAM T.	
	Examiner Michael R Vaughan	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _27 June 2002_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-36_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-36_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _21 September 2000_ is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _2-4_.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Claims 1-36 have been examined and are pending.

Information Disclosure Statement

An initialed and dated copy of Applicant's IDS form 1449, Paper No. 2-4, is attached to the instant Office action.

Claim Objections

Claims 23 and 25 are objected to because they are the exact same limitation and both are dependents of claim 22.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-34 are rejected under 35 U.S.C. 101 because the language of the independent claims 1, 6, 14, 28, and 33 raises a question as to whether the claim is directed merely to an abstract idea that is not tied to a technological art, environment, or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 USC 101. There is nothing in any of the independent claims that would tie the algorithm to a particularly physical device such as a computer. The independent claims recite steps that could be performed by hand.

Claim Rejections - 35 USC ' 112, second paragraph

Claim 6 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 6 discloses that each pair of keys has a corresponding token. However, in the second step of transmitting the set of key pairs to the receiver, the corresponding token is also sent. "[T]he corresponding token" lends itself to being only one token when there are many. Examiner is assuming that each token is being sent so on the merits claim 6 will be interpreted as –transmitting the set of N cryptogram/decryption key pairs and the corresponding token<u>s</u> to a receiver--. Clarification and/or correction are required.

Claim Rejections - 35 USC ' 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Merkle (Secure Communications Over Insecure Channels) in view of Johnson et al, herein Johnson, (USP 5,815,573).

As per claim 1, Merkle teaches creating a set of N trap door encryption-decryption function pairs each paired with a corresponding token; transmitting the set of N trap door encryption-decryption function pairs along with a corresponding token to a receiver; randomly selecting at the receiver one of the trap door encryption-decryption function pairs and the corresponding token; recording in a key escrow database the created set of N trap door encryption decryption function pairs and the corresponding paired token; recording in the key escrow database the randomly selected trap door encryption decryption function pair along with the encrypted token; and inverting the created set of N trap door encryption-decryption function pairs and the randomly selected trap door encryption-decryption function pair along with the encrypted token to identify the decryption key (pages 296-299). Merkle is silent in explicitly disclosing adding randomization information at the receiver to the corresponding token of the selected trap door encryption-decryption function pair and encrypting the token with the added randomization information, the token corresponding with the randomly selected encryption-decryption function pair.

Johnson teaches adding randomization information at the receiver to the corresponding token of the selected trap door encryption-decryption function pair and encrypting the token with the added randomization information, the token corresponding with the randomly selected encryption-decryption function pair (column 7, lines 54-64 and column 9, lines 1-60). In Merkle the token is sent back in the clear. Johnson teaches adding randomized values to the token to increase the difficulty of gaining any useful knowledge from the communication. In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Johnson within the system of Merkle because it would prevent the token from being sent in the clear over an unsecure channel.

As per claim 6, Merkle teaches generating, in accordance with a selected encryption function, a set of N cryptogram/decryption key pairs, each pair having a corresponding token; transmitting the set of N cryptogram/decryption key pairs and the corresponding token to a receiver; randomly selecting at the receiver one of the cryptogram/decryption key pairs along with the corresponding token; decrypting the randomly selected cryptogram utilizing the corresponding token to obtain a corresponding decryption key; generating a cryptogram utilizing the corresponding decryption key and comprising the selected token; recording in an escrow database the generated set of N cryptogram/decryption key pairs along with each corresponding token and the generated cryptogram based on the randomly selected cryptogram/decryption key pair; and inverting the recorded set of N cryptogram/decryption key pairs and the generated cryptogram to identify a decryption key from the key escrow database (pages 296-299).

Merkle is silent in explicitly teaching using randomized to generate a cryptogram. Johnson teaches adding randomization information at the receiver to the corresponding token of the selected trap door encryption-decryption function pair and encrypting the token with the added randomization information, the token corresponding with the randomly selected encryption-decryption function pair (column 7, lines 54-64 and column 9, lines 1-60). In Merkle the token is sent back in the clear. Johnson teaches adding randomized values to the token to increase the difficulty of gaining any useful knowledge from the communication. In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Johnson within the system of Merkle because it would prevent the token from being sent in the clear over an unsecure channel.

As per claim 14, Merkle teaches a method for secure communication between an originator and a receiver using message encryption, comprising: creating at an originator a set of N trap door functions each paired with a corresponding token, each trap door function comprising a cryptogram/decryption key pair; transmitting the set of N trap door functions to a receiver; randomly selecting at the receiver one of the trap door functions and the corresponding token (page 296-297); encrypting at the receiver the decryption key with the randomly selected trap door function; transmitting the encrypted decryption key with the randomly selected trap door function to the originator (page 298); and decoding the encrypted decryption key with the randomly selected trap door function utilizing originator retained trap door information.

Merkle is silent in explicitly teaching using randomized to generate a cryptogram. Johnson teaches adding randomization information at the receiver to the corresponding token of the selected trap door encryption-decryption function pair and encrypting the token with the added randomization information, the token corresponding with the randomly selected encryption-decryption function pair (column 7, lines 54-64 and column 9, lines 1-60). In Merkle the token is sent back in the clear. Johnson teaches adding randomized values to the token to increase the difficulty of gaining any useful knowledge from the communication. In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Johnson within the system of Merkle because it would prevent the token from being sent in the clear over an unsecure channel.

As per claim 28, Merkle teaches a method for storing and withdrawing a decryption key from a key escrow database, comprising: creating a set of N trap door encryption-decryption function pairs each paired with a corresponding token;

transmitting the set of N trap door encryption-decryption function pairs along with a corresponding token to a receiver; randomly selecting at the receiver one of the trap door encryption-decryption function pairs and the corresponding token; the token corresponding with the randomly selected encryption-decryption function pair; recording in a key escrow database the created set of N trap door encryption decryption function pairs and the corresponding paired token; recording in the key escrow database the randomly selected trap door encryption decryption function pair along with the encrypted token and the added randomization information; retrieving from the key escrow database the created set of N trap door encryption decryption function pairs and the corresponding pair token, and the randomly selected trap door encryption-decryption function pair along with the encrypted token and the added randomization information; and inverting the created set of N trap door encryption-decryption function pairs and the randomly selected trap door encryption-decryption function pair along with the encrypted token and the added randomization information to identify the decryption key (pages 296-299).

Merkle is silent in explicitly teaching using randomized to generate a cryptogram. Johnson teaches adding randomization information at the receiver to the corresponding token of the selected trap door encryption-decryption function pair and encrypting the token with the added randomization information, the token corresponding with the randomly selected encryption-decryption function pair (column 7, lines 54-64 and column 9, lines 1-60). In Merkle the token is sent back in the clear. Johnson teaches adding randomized values to the token to increase the difficulty of gaining any useful knowledge from the communication. In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Johnson within the system of Merkle because it would prevent the token from being sent in the clear over an unsecure channel.

As per claim 33, Merkle teaches a method for storing and withdrawing decryption keys from a key escrow database, comprising: generating, in accordance with a selected encryption function, a set of N cryptogram/decryption key pairs, each pair having a corresponding token; transmitting the set of N cryptogram/decryption key pairs and the corresponding token to a receiver; randomly selecting at the receiver one of the cryptogram/decryption key pairs along with the corresponding token; decrypting the randomly selected cryptogram utilizing the corresponding token to obtain a corresponding decryption key; generating a cryptogram utilizing the corresponding decryption key and comprising the selected token; recording in an escrow database the generated set of N cryptogram/decryption key pairs along with each corresponding token; recording in an escrow database the generated cryptogram based on the randomly selected cryptogram/decryption key pair; retrieving from the key escrow database the generated set of N cryptogram/decryption key pairs along with each corresponding token, and the generated cryptogram based on the randomly selected cryptogram/decryption key pair; and inverting the recorded set of N cryptogram/decryption key pairs and the generated cryptogram to identify a decryption key from the key escrow database.

Merkle is silent in explicitly teaching using randomized to generate a cryptogram. Johnson teaches adding randomization information at the receiver to the corresponding token of the selected trap door encryption-decryption function pair and encrypting the token with the added randomization information, the token corresponding with the randomly selected encryption-decryption function pair (column 7, lines 54-64 and column 9, lines 1-60). In Merkle the token is sent back in the clear. Johnson teaches adding randomized values to the token to increase the difficulty of gaining any useful knowledge from the communication. In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Johnson within the system of Merkle because it would prevent the token from being sent in the clear over an unsecure channel.

As per claims 2 and 29, Merkle teaches encrypting the created set of N trap door encryption-decryption function pairs and the randomly selected trap door function along with the decryption key prior to recording in the key escrow database (page 298).

As per claims 3, 7, 14, 30 and 36, Merkle does not explicitly teach the receiver selecting more than one of the puzzles to decrypt. Clearly from the teachings of Merkle one of ordinary skill in the art would know that the work needed to be performed by an eavesdropper plotting to learn the decryption key is O(n^2). Having the receiver choose more than one puzzles slightly increases the poor security of Merkle's system by forcing the eavesdropper to perform more calculations. The limitations of claim 3 are merely repeating an already disclosed limitation that does not produce an unobvious result. The examiner supplies the same rationale then for incorporating the suggestions of Johnson et al's system to then further randomize each token as recited in the rejection of claim 1.

As per claims 4, 5, 31 Merkle teaches using identifying information to distinguish when puzzles have been correctly solved (page 296). Merkle does teach the use of a digital signature. Merkle does teach that keys are looked up based upon a user (page 298). Therefore there is a need to have a positively identifying means to ascertain the correct author of a published key. Johnson et al teaches the use of a digital signature (column 10, lines 61-63). In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Johnson et al within the system of Merkle because it would associate a key to a user with provable certainty.

As per claim 8, Merkle teaches decrypting the cryptogram of a cryptogram/decryption key pair using the associated decryption key to identify token information (page 299).

As per claim 9, Merkle does not teach explicitly using a linear transformation to combine the token information. Johnson teaches the use of linear transformation to add keys together (figure 1, element 110). In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Johnson et al within the system of Merkle because linear transforms are a fast well established operation in order to carry out transformations.

As per claim 10, Merkle teaches the utilization of a symmetrical cryptosystem (page 296).

As per claim 11, Merkle teaches the utilization of a public key cryptosystem (page 299).

As per claims 12 and 35, Merkle teaches wherein recording in an escrow database further comprises encrypting the generated set of N cryptogram/decryption key pairs and a response message from the receiver prior to recording (page 296).

As per claims 13 and 21, Merkle teaches using identifying information to distinguish when puzzles have been correctly solved (page 296). Merkle does teach the use of a digital signature. Merkle does teach that keys are looked up based upon a user (page 298). Therefore there is a need to have a positively identifying means to ascertain the correct author of a published key. Johnson et al teaches the use of a digital signature (column 10, lines 61-63). In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Johnson et al within the system of Merkle because it would associate a key to a user with provable certainty.

As per claim 15, Merkle teaches decrypting at the receiver the cryptogram to identify the corresponding token utilizing the decryption key of the cryptogram/decryption key pair (page 296).

As per claims 16 and 32, Merkle teaches encrypting at the receiver an escrow key comprises generating a cryptogram comprising; the corresponding token, the decryption key and randomization information (page 298).

As per claim 17, Merkle teaches decoding the encrypted escrow key comprises selecting a decryption key randomly from a selected group of decryption keys (page 296).

As per claim 18, Merkle teaches comprising recognizing a correct decoding result utilizing structural information embedded in the response message (page 296).

As per claim 19, Merkle teaches creating at an originator further comprises generating the set of N trap door functions utilizing a selected encryption function and a private encryption key (page 297).

As per claims 24 and 34, Merkle does not explicitly teach the receiver selecting more than one of the puzzles to decrypt. Clearly from the teachings of Merkle one of ordinary skill in the art would know that the work needed to be performed by an eavesdropper plotting to learn the decryption key is O(n^2). Having the receiver choose more than one puzzles slightly increases the poor security of Merkle's system by forcing the eavesdropper to perform more calculations. The limitations of claim 3 are merely repeating an already disclosed limitation that does not produce an unobvious result. The examiner supplies the same rationale then for incorporating the suggestions of Johnson et al's system to then further randomize each token as recited in the rejection of claim 14. Merkle teaches encrypting at the receiver an escrow key comprises generating a cryptogram comprising; the corresponding token, the decryption key and randomization information (page 298).

As per claim 23 and 25, Merkle teaches the utilization of a symmetrical cryptosystem (page 296).

As per claim 24, Merkle teaches the utilization of a public key cryptosystem (page 299).

As per claim 26, Merkle teaches recording in an escrow database the created N trap door functions along with each corresponding token and the encrypted escrow key with the randomly selected trap door function (page 298).

As per claim 27, Merkle teaches inverting the recorded set of N trap door functions and the encrypted escrow key with the randomly selected trap door function to identify a decryption key from the key escrow database (page 297 and 298).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MV
Michael R Vaughan

Examiner

Art Unit 2131

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100